PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-129441
(43)Date of publication of application : 30.04.1992

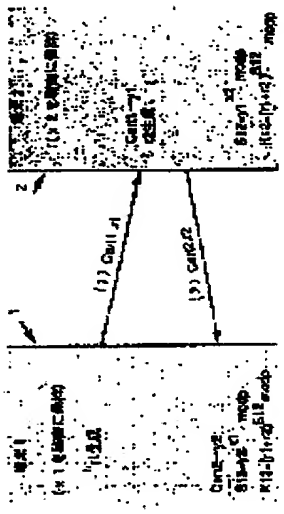
(51)Int.CI. H04L 9/28
G09C 1/00

(21)Application number : 02-253156
(22)Date of filing : 20.09.1990

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : MATSUZAKI NATSUME
TATEBAYASHI MAKOTO
HARADA TOSHIHARU

(54) KEY DELIVERY METHOD WITH VERIFICATION FUNCTION

(57)Abstract:
PURPOSE: To reduce number of times for key delivery and to save quantity of calculation for obtaining a common key by generating the common key according to a power based on a certificate sent from an opposite party and fixed secret information between both terminal equipments and according to a root residual of a random number generated from both the terminal equipments.
CONSTITUTION: Terminal equipments 1, 2 generate random numbers r1, r2 respectively and send them to the terminal equipments 2,1 together with their own certificates Cert1, Cert2. Then the two terminal equipments 1,2 use an open inverse variable (h) to obtain root residuals y1, y2 of the opposite terminal equipments from the certificates Cert1, Cert2 sent from the opposite terminal equipments, calculate root residual operators S12, S21 of the root residuals y1, y2 of the opposite terminal equipments by using own secret information x1, x2 as a power, apply a prescribed calculation by using random numbers r1, r2 of both the terminal equipments 1,2 to generate common keys K12, K21 through the use of the root residuals S12, S21 as the power. Thus, the key delivery with a verification function is implemented with less number of times of communication and less calculation quantity to obtain the common key.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平4－129441

⑤Int. Cl.⁵	識別記号	庁内整理番号	⑬公開 平成4年(1992)4月30日
H 04 L 9/28 G 09 C 1/00		7922－5L 7117－5K　H 04 L 9/02　A	

審査請求　未請求　請求項の数 2　（全10頁）

⑭発明の名称　認証機能付き鍵配送方法

⑳特　願　平2－253156
㉒出　願　平2(1990)9月20日

㉑発明者　松崎　なつめ　大阪府門真市大字門真1006番地　松下電器産業株式会社内
㉑発明者　舘林　誠　大阪府門真市大字門真1006番地　松下電器産業株式会社内
㉑発明者　原田　俊治　大阪府門真市大字門真1006番地　松下電器産業株式会社内
㉑出願人　松下電器産業株式会社　大阪府門真市大字門真1006番地
㉔代理人　弁理士　中島　司朗

明　細　書

1．発明の名称

認証機能付き鍵配送方法

2．特許請求の範囲

(1) 重複しない固有の識別情報を持った複数の端末と、各端末が作成した公開情報に署名を施して証明書を発行するセンターからなるシステムにおいて、

各端末が公開の数pとこのpを法とする剰余環の原始元gを用いて、各端末固有の秘密情報x_1，x_2…をべきとし前記pを法とするgのべき乗剰余演算値y1，y2…を算出し、センターに送るステップと、

センターが前記算出値に秘密変換fを施して証明書Cert1、Cert2…を生成し、各端末に配付するステップと、

共通の鍵を持つことを所望する2つの端末の一方が自己の生成する乱数r_1と証明書Cert1をもう一方の端末に送るステップと、

もう一方の端末が自己の生成する乱数r_2と証明書Cert2を前記一方の端末に送るステップと、

前記2つの端末が、公開の逆変換hを用いて相手端末から送られた証明書Cert1、Cert2から相手端末の前記べき乗剰余演算値y1，y2を求めるステップと、

自己の秘密情報x1，x2をべきとし、公開の数pを法とする相手端末の前記y2，y1のべき乗剰余演算値S12、S21を算出するステップと、

双方の端末の乱数r_1，r_2を用いて所定の演算を行い共通の結果r12，r21を得るステップと、

前記べき乗剰余演算値S12，S21をべきとし、公開の数pを法とする前記r12，r21のべき乗剰余演算を行って双方の端末で共通の鍵K12，K21を生成するステップと、

から成る双方向通信の認証機能付き鍵配送方法。

(2) 重複しない固有の識別情報を持った複数の端末と、各端末が作成した公開情報に署名を施して証明書を発行するセンターとからなるシステムにお

いて、

各端末が公開の数ｐとこのｐを法とする剰余環の原始元ｇを用いて、各端末固有の秘密情報ｘ１，ｘ２…をべきとし前記ｐを法とするｇのべき乗剰余演算値ｙ１，ｙ２…を算出し、センターに送るステップと、

センターが前記算出値に変換ｆを施して証明書Cert１、Cert２…を生成し、公開リストに登録するステップと、

発信側端末が、自己の生成した乱数ｒ１をべきとし前記公開の数ｐを法とした前記ｇのべき乗剰余演算値Ｚ１を計算するステップと、

発信側端末において公開リストを参照し特定の受信側端末の証明書Cert２に公開の逆変換ｈを施して受信側端末のべき乗剰余演算値ｙ２を得るステップと、

発信側端末において自己の生成した乱数ｒ１をべきとし、公開の数ｐを法とする前記ｙ２のべき乗剰余値ｕ１を計算するステップと、

発信側端末において自己の生成した秘密情報ｘ１をべきとし、公開の数ｐを法とする前記ｙ２のべき乗剰余値Ｓ１２を算出するステップと、

前記ｕ１とＳ１２を用いて受信側端末との共有鍵を生成するステップと、

前記共有鍵を公開の一方向性関数に入力して出力ｖ１を得るステップと、

発信側端末の証明書Cert１、前記Ｚ１、及びｖ１を受信側端末に送付するステップと、

受信側端末において、発信側端末の証明書Cert１に公開の逆変換ｈを施してべき乗剰余演算値ｙ１を得るステップと、

受信側端末において自己の生成した秘密情報ｘ２をべきとし、公開の数ｐを法とする前記Ｚ１のべき乗剰余値ｕ２を計算するステップと、

前記秘密情報ｘ１をべきとし、公開の数ｐを法とする前記ｙ１のべき乗剰余値Ｓ２１を算出するステップと、

前記ｕ２とＳ２１を用いて発信側端末との共有鍵を生成するステップと、

前記共有鍵を公開の一方向性関数に入力して出力ｖ２を得るステップと、

前記ｖ２を発信側端末から送付されたｖ１と比較し、一致しているときのみ受信側端末において生成した共有鍵を有効と決定するステップと、

から成る一方向通信の認証機能付き鍵配送方法。

3．発明の詳細な説明

産業上の利用分野

本発明は、各端末が生成した公開情報に、信頼の於けるセンターがあらかじめ署名を施した証明書を用いて、自分の認識している相手とのみ同じ鍵を共有できる認証機能付き鍵配送方法に関する。

従来の技術

複数の端末が接続された通信網において、他の端末に秘密の状態で特定の端末間で通信を行いたい要望がある。このような要望は双方向通信の場合だけでなく、電子メールのような一方向通信の場合も同様である。

上記要望に応じる手法として、秘密通信を希望する２つの端末間で共通の鍵を持ち、送信側がこの鍵を用いて送信情報に施錠して送信し、受信側が共通鍵を用いて受信情報を解錠するという方法がある。

この場合、２つの端末間で共有する鍵は、他の端末に対して秘密でなければならない。このような秘密鍵を２つの端末間で共有できるようにする一手法として公開鍵配送法（public key distribution system:PKDS）という方法がある。

この方法は、通信網の利用者が公開鍵を用いて秘密鍵を共有する方法である。秘密鍵暗号を適用する場合、秘密鍵自体を安全でない通信路を介して配送するわけにはいかず、まえもって何らかの安全な手段（例えば、密使や書留郵便など）で通信相手と秘密鍵を共有する必要がある。ところが、公開鍵配送法を用いると、安全でない（盗聴されてもかまわない）通信路を介して共有の秘密鍵を生成できる。公開鍵配送法では、通信相手同士が公開鍵を交換して計算した結果、この両者のみが知り得るランダムな秘密鍵の値が生成され、それを共有の秘密鍵に用いるのである。

なお、鍵配送と同時に、鍵を共有する相手をき

ちんと認証することも要望される。この認証がなされないと、鍵を共有している相手が真に秘密通信を希望する相手と同一であるかどうかが確認できないからである。

従って、ここでは認証機能を組込んだ公開鍵配送法について説明する。

公開鍵配送方法として、１９７６年にDiffieとHellman によって提案されたＤＨ鍵配送方式がある。これは、有限体ＧＦ（ｐ）上での離散対数問題が難しいことに安全性の根拠をおいている。これに認証機能を組み込むため、信頼のおけるセンター発行の証明書を用いた方法が提案されている。（説明の便宜上この方法もＤＨ鍵配送方式と呼ぶ）

以下、ＤＨ鍵配送方式の手順をセンターによる証明書の発行のフェーズと、端末１と端末２の間の鍵配送のフェーズに分けて説明する。

〔証明書の発行フェーズ〕

(1) システムの構築時、法ｐとＧＦ（ｐ）の原始元ｇを決定し各端末に公開する。

(2) 端末１は秘密情報ｘ１を生成して、$y1=g^{x1}\bmod p$を計算する。　…(1)

なお、ここで' X　mod p' は値Ｘをｐで除した時の剰余を示す。

(3) 端末１はｙ１と名前、住所など自分を特定できる情報（識別情報、又はＩＤ情報と称する）ＩＤ１を信頼のおけるセンターに送信し、証明書を請求する。

(4) センターは端末１の正当性を調べ、センターだけが知っている秘密変換ｆを用いて、証明書Cert1を生成し、例えば磁気カードＦ等に格納して端末１に配付する。

Cert1＝ｆ（ｙ１||ＩＤ１）

ここで、||は連結を示している。なお、秘密変換ｆの逆変換ｈはシステムにおいて公開であるとする。従って、Cert1を得た任意の端末はｈ（Cert1）を計算することによってセンターによって保証されたＩＤ１の公開情報ｙ１を得ることができる。

〔鍵配送フェーズ〕

(1) 端末１は自身の証明書Cert1を端末２に、端末２は自身の証明書Cert2をそれぞれ配送する。

(2) 端末１はｈ（Cert2）＝ｙ２||ＩＤ２を計算し、自分の秘密情報ｘ１を用いて、

$K12=y2^{x1}\bmod p=g^{x1\times x2}\bmod p$

を求める。

(3) 一方、端末２はｈ（Cert1）＝ｙ１||ＩＤ１を計算し、自分の秘密情報ｘ２を用いて、

$K21=y1^{x2}\bmod p=g^{x1\times x2}\bmod p$

を求める。なお、Ｋ１２＝Ｋ２１は端末１と２の間の共有鍵である。

ところで、通信で用いられる鍵は、安全上時々変更することが望ましい。上記で述べたＤＨ鍵配送方式では共有鍵を変更するのにもう一度センターに依頼して証明書を発行してもらう必要があり、非常に手間である。

そこで、証明書は変更せずに共有鍵を変更する方法がいくつか提案されている。

以下、従来提案されている２つの方法について説明する。

〔方法１（第１の従来例）〕

方式１は、「山元・秋山"ア　データ　エンクリプション　デバイス　インコーポレイティング　ファスト　ピーケイディエス"(A Data Encryption device incorporation fast PKDS",Global Com.,32.2.1-32.2.6(Dec.1983)」で提案されている方法である。

証明書の発行フェーズはＤＨ鍵配送方式と同じである。

第３図は鍵配送フェーズの手順を示している。１は秘密情報ｘ１を保持する端末１、２は秘密情報ｘ２を保持する端末２である。以下に動作を示す。

(1) 端末１は端末２に自分の証明書Cert1を送付する。

(2) 端末２は、ｈ（Cert1）を計算して端末１の正規の公開情報ｙ１を得る。

また、次のようにして配送情報Ｚ２１を生成し、これと自分の証明書Cert2を端末１に送付する。

(a) 乱数ｒ２を発生する。

(b) $Z21 = y1^{x2 \times r2} \bmod p$ …(2)

(3) 端末1は、h (Cert2) を計算して端末2の正規の公開情報y2を得る。

また、次のようにして配送情報Z12を生成し、これを端末2に送付する。

(a) 乱数r1を発生する。

(b) $Z12 = y2^{x1 \times r1} \bmod p$ …(3)

そして、端末2からの配送情報Z21を用いて共有鍵K12を生成する。

$K12 = Z21^{r1} \bmod p$

(4) 端末2は、端末1からの配送情報Z12を用いて共有鍵K21を生成する。

$K21 = Z12^{r2} \bmod p$

なお、端末1における共有鍵K12と端末2における共有鍵K21は(1)～(3)式より同じになる。

$K12 = Z21^{r1} \bmod p = y1^{x2 \times r2 \times r1} \bmod p$

$= g^{x1 \times x2 \times r1 \times r2} \bmod p$

$K21 = Z12^{r2} \bmod p$

$= y2^{x1 \times r1 \times r2} \bmod p$

$= g^{x1 \times x2 \times r1 \times r2} \bmod p$

ところで、この方法は配送情報を生成するために相手の証明書が必要であるため、3パス（片道）の通信が必要となる。

〔方法2（第2の従来例）〕

方法2は、「岡本・中村"公開鍵配送方式の一検討"昭和59年度電子通信学会全国大会、15」で提案されている方法である。

証明書の発行フェーズはDH鍵配送方式と同じである。

第4図に鍵配送フェーズの手順を示している。端末1、2間の動作を以下に示す。

(1) 端末1は次のようにして配送情報Z12を生成し、これと自分の証明書Cert1を端末2に送付する。

(a) 乱数r1を発生する。

(b) $Z12 = y1^{r1} \bmod p$ …(4)

(2) 端末2は次のようにして配送情報Z21を生成し、これと自分の証明書Cert2を端末1に送付する。

(a) 乱数r2を発生する。

(b) $Z21 = y2^{r2} \bmod p$ …(5)

また、端末1から送付されてきた情報を用いて、以下のとおり共有鍵K21を生成する。

(a) Cert1より、h (Cert1) = y1 | | ID1を得る。

(b) 端末1からの配送情報Z12より次のように共有鍵を算出する。

$K21 = (Z12 \times y1^{r2})^{x2} \bmod p$

(3) 端末1は、端末1からの配送情報を用いて共有鍵K12を生成する。

$K12 = (Z21 \times y2^{r1})^{x1} \bmod p$

なお、端末1における共有鍵K12と端末2における共有鍵K21は(4)(5)式より同じになる。

$K12 = (Z21 \times y2^{r1})^{x1} \bmod p$

$= (y2^{r2 \cdot r1})^{x1} \bmod p$

$= g^{x1 \times x2 (r1 \cdot r2)} \bmod p = k21$

この方法は配送情報を生成するために相手の証明書が不要であるため、2回の通信で鍵配送を行うことができる。また、共有鍵の生成に正規の端末の秘密情報が必要であるため、正規の端末対のみが同じ鍵が共有できる間接的認証付きの鍵配送方式になっている。しかしながら、この方法では各端末は配送情報の生成に1回、共有鍵の生成に2回の計3回のべき乗剰余演算が必要となる。

また、電子メールのような一方向通信への応用においては、一方向の通信で認証付きの鍵配送を行うことが必要になる。この場合、前述のセンター発行の証明書をネットワークのセンターが公開リストとして管理しておき、送信者がこれを参照することを前提とする。

次に、DH鍵配送方式を基本にして、一方向通信において共有鍵を毎回変更できる方法を説明する。

第5図に鍵配送フェーズの手順を示している。以下端末1、2の動作について述べる。

(1) 端末1は乱数r1を生成して、これと自分の証明書Cert1を端末2に送信する。

(2) 端末1は公開リストから端末2の証明書Cert2を参照し、h (Cert2) = y2 | | ID2を得る。

端末１は以下の計算を行い端末２との共有鍵を得る。

Ｓ１２＝ｙ２^ｘ１ modp

Ｋ１２＝Ｆ（ｒ１、Ｓ１２）

ここにおいてＦ（）はあらかじめ定められた演算である。従って、例えば

Ｆ（ｘ、ｙ）＝ｘ＋ｙ　modp

とすると、Ｋ１２＝ｒ１＋Ｓ１２ modpとなる。

(3) 端末２は端末１から送付された端末１の証明書Cert１からｙ１を得る。

端末２は端末１から送付された乱数ｒ１を用いて以下の計算を行い端末１との共有鍵を得る。

Ｓ２１＝ｙ１^ｘ２ modp

Ｋ２１＝Ｆ（ｒ１、Ｓ２１）

＝ｒ１＋Ｓ２１ modp

なお、ここでＳ１２＝Ｓ２１＝ｇ^ｘ１ｘ２であるため、Ｋ１２＝Ｋ２１がなりたつ。

発明が解決しようとする課題

以上のように双方向通信バージョンの第１の従来例では、配送情報の生成に相手の証明書を用いるため、最低３パス（片道）の通信が必要となる。また、第２の従来例では共有鍵を求めるための計算量が大である。

また、一方向通信バージョンの従来例には以下の問題点がある。例えば、Ｆ（ｘ、ｙ）＝ｘ＋ｙ modpの場合、あるセッションにおける共有鍵Ｋ１２とその時の通信路上のデータｒ１が、第３者に一旦求められてしまうと、Ｓ１２＝Ｋ１２－ｒ１ modpによって第３者は端末１と２の間の固定の共有鍵Ｓ１２を得る。そして、任意のセッションにおける通信路上のデータを観測し、得たＳ１２を用いれば、端末１と２の間の任意の共有鍵を求めることができる。つまり、そのセッションだけに有効であるためにあまり守秘に重きをおいていない共有鍵から、大切な固定の共有秘密鍵が求められてしまう。

本発明は上述の問題点に鑑み、双方向通信において、鍵配送時の端末間の通信回数を減少して鍵共有に必要となる計算量を削減した認証機能付き鍵配送方法を提供することを第１の目的とする。

本発明の第２の目的は、一方向通信において、第３者がセッション鍵から固定鍵を求めることが困難であり、また、受信者が発信者の認証を行う認証機能付き鍵配送方法を提供することである。

課題を解決するための手段

第１の目的を達成するため、本発明は、重複しない固有の識別情報を持った複数の端末と、各端末が作成した公開情報に署名を施して証明書を発行するセンターからなるシステムにおいて、各端末が公開の数ｐとこのｐを法とする剰余環の原始元ｇを用いて、各端末固有の秘密情報ｘ１，ｘ２…をべきとし前記ｐを法とするｇのべき乗剰余演算値ｙ１，ｙ２…を算出し、センターに送るステップと、センターが前記算出値に秘密変換ｆを施して証明書Cert１、Cert２…を生成し、各端末に配付するステップと、共通の鍵を持つことを所望する２つの端末の一方が自己の生成する乱数ｒ１と証明書Cert１をもう一方の端末に送るステップと、もう一方の端末が自己の生成する乱数ｒ２と証明書Cert２を前記一方の端末に送るステップと、前記２つの端末が、公開の逆変換ｈを用いて相手端末から送られた証明書Cert１、Cert２から相手端末の前記べき乗剰余演算値ｙ１，ｙ２を求めるステップと、自己の秘密情報ｘ１，ｘ２をべきとし、公開の数ｐを法とする相手端末の前記ｙ２，ｙ１のべき乗剰余演算値Ｓ１２、Ｓ２１を算出するステップと、双方の端末の乱数ｒ１，ｒ２を用いて所定の演算を行い共通の結果ｒ１２，ｒ２１を得るステップと、前記べき乗剰余演算値Ｓ１２，Ｓ２１をべきとし、公開の数ｐを法とする前記ｒ１２，ｒ２１のべき乗剰余演算を行って双方の端末で共通の鍵Ｋ１２，Ｋ２１を生成するステップと、から成ることを特徴としている。

第２の目的を達成するため、本発明は重複しない固有の識別情報を持った複数の端末と、各端末が作成した公開情報に署名を施して証明書を発行するセンターとからなるシステムにおいて、各端末が公開の数ｐとこのｐを法とする剰余環の原始元ｇを用いて、各端末固有の秘密情報ｘ１，ｘ２…をべきとし前記ｐを法とするｇのべき乗剰余演

算値ｙ１，ｙ２…を算出し、センターに送るステップと、センターが前記算出値に変換ｆを施して証明書Cert１、Cert２…を生成し、公開リストに登録するステップと、発信側端末が、自己の生成した乱数ｒ１をべきとし前記公開の数ｐを法とした前記ｇのべき乗剰余演算値Ｚ１を計算するステップと、発信側端末において公開リストを参照し特定の受信側端末の証明書Cert２に公開の逆変換ｈを施して受信側端末のべき乗剰余演算値ｙ２を得るステップと、発信側端末において自己の生成した乱数ｒ１をべきとし、公開の数ｐを法とする前記ｙ２のべき乗剰余値ｕ１を計算するステップと、発信側端末において自己の生成した秘密情報ｘ１をべきとし、公開の数ｐを法とする前記ｙ２のべき乗剰余値Ｓ１２を算出するステップと、前記ｕ１とＳ１２を用いて受信側端末との共有鍵を生成するステップと、前記共有鍵を公開の一方向性関数に入力して出力ｖ１を得るステップと、発信側端末の証明書Cert１、前記Ｚ１、及びｖ１を受信側端末に送付するステップと、受信側端末において、発信側端末の証明書Cert１に公開の逆変換ｈを施してべき乗剰余演算値ｙ１を得るステップと、受信側端末において自己の生成した秘密情報ｘ２をべきとし、公開の数ｐを法とする前記Ｚ１のべき乗剰余値ｕ２を計算するステップと、前記秘密情報ｘ１をべきとし、公開の数ｐを法とする前記ｙ１のべき乗剰余値Ｓ２１を算出するステップと、前記ｕ２とＳ２１を用いて発信側端末との共有鍵を生成するステップと、前記共有鍵を公開の一方向性関数に入力して出力ｖ２を得るステップと、前記ｖ２を発信側端末から送付されたｖ１と比較し、一致しているときのみ受信側端末において生成した共有鍵を有効と決定するステップと、から成ることを特徴としている。

作用

第１の発明では、相手の証明書と双方の端末間において固定の秘密情報Ｓ１２をべきとし、双方の端末が発生した乱数のべき乗剰余値を、共有鍵としている。従って、鍵からそのべき部の固定の秘密情報Ｓ１２を求めることは困難である。配送情報は自身の発生した乱数だけであり、また、共有鍵の計算にはそれぞれの端末で１回のべき乗剰余演算を行えばよいため、鍵配送のための通信回数・鍵共有のための計算量共に削減される。

第２の発明では、第３者が送信者に成りすましてセッション鍵から固定の共有鍵を求める不正を防ぐために、ｖ１＝ｖ２により送信者の認証を行っている。また、もしＳ１２が得られた場合も、共有鍵の送受信者だけで共有できるセッション毎のデータｕ１－ｕ２を用いることによって、自分自身が送信者になりすます以外には、セッション鍵は得られない。

実施例

第１図は、双方向通信を行う本発明の認証機能付き鍵配送方法の一実施例を示す。１は秘密情報ｘ１を保持する第１の端末、２は秘密情報ｘ２を保持する第２の端末である。なお、実際には端末１、２だけでなく、複数の端末及びセンターが通信回線に接続された構成のシステムであるが、ここでは簡単のため、共通の鍵をもつことを希望する２つの端末１、２だけを示す。また、証明書発行フェーズは従来例と同じなので説明は省略し、鍵配送フェーズについてステップ毎に図を用いて説明する。

ステップ(1)：

端末１は乱数ｒ１を生成し、自分の証明書Cert１と共に端末２に送信する。

ステップ(2)：

端末２は乱数ｒ２を生成し、自分の証明書Cert２と共に端末２に送信する。

ステップ(3)：

端末１は端末２から送信された証明書Cert２から、

$h(Cert2) = y2 \| ID2$

を計算し、相手が端末２であることを確認する。

ステップ(4)：

次に、上記ｙ２と自分の秘密情報ｘ１を用いて

$S12 = y2^{x1} \bmod p$

を計算する。

なお、このＳ１２は端末１、２間の固定の共有データである。

ステップ(5)：

そして、端末2から送信された乱数r2と自分が生成した乱数r1、上記S12を用いてこのセッションにおける端末2との共有鍵K12を計算する。この時、S12を共有鍵のべきの部分に用いる。

$K12=(r1+r2)^{S12} \bmod p$

ステップ(6)：

端末2は端末1から送信された証明書Cert1から、

h(Cert1)=y1||ID1

を計算し、相手が端末2であることを確認する。

ステップ(7)：

次に、上記y1と自分の秘密情報x2を用いて、$S21=y1^{x2} \bmod p$ を計算する。

なお、このS21は端末1、2間の固定の共有データであり、上記S12と同じ値である。

$S12=S21=g^{x1 \times x2} \bmod p$

ステップ(8)：

そして、端末1から送信された乱数r1と自分が生成した乱数r2、上記S21を用いてこのセッションにおける端末2との共有鍵K21を計算する。この時、S12を共有鍵のべきの部分に用いる。

$K21=(r1+r2)^{S21} \bmod p$

なお、S12=S21よりK12=K21が成り立つ。

この実施例からわかるように、S12(=S21)を得るためには、正規の端末の秘密情報が必要である。このため、正規の端末だけが共通の鍵を得ることができる。それ故、この実施例は間接的な認証付きの鍵配送方法であるといえる。

なお、相手を確実に確認するためには、共通の鍵を算出できたことを示せばよい。これには例えば一方向性の関数f()を定め、これにそれぞれの端末で得た共通鍵を入力したときの出力値を交換する。つまり、端末1はf(K12、ID1)を端末2に送付し、端末2ではこれをf(K21、ID1)と比較する。また、端末2はf(K21、ID2)を端末1に送付し、端末1ではこれをf(K12、ID2)と比較する。そしてこのことによってそれぞれ相手を認証する。

また、セッション鍵は端末1、2の共有データ(固定値)をべきとし、pを法とした端末1、2が生成した乱数のべき乗剰余値(セッションごとに異なる数値)である。従って、セッション鍵と通信路上のデータから、べきの部分である秘密の共有データ(固定値)を求めるには、GF(p)上の離散対数問題をとく必要があり、pの数を例えば1000ビット程度に設定することによって計算量的に安全になる。

そして共有鍵を得るには、S12の算出に1回、共有鍵の算出に1回の計2回のべき乗剰余演算が必要である。

なお、この実施例では端末1、2で発生した乱数r1、r2からセッション毎に異なる数値を求めるに加算を用いているが、あらかじめ定められたものであればこの演算R()はどのようなものであってもよい。ただし、トータルの計算量の削減のためには加算又は乗算などが適している。

ただし、例えばR(x、y)=x+y modpの場合、次のような攻撃が可能となりうる。

(1) 第3者端末3は、正規の端末1、端末2間の通信を盗聴する。

(2) 端末1からは乱数r1と証明書Cert1が送信される。

(3) 端末3は、r1+r3=1 modpを満たす、r3を算出する。

(4) 端末3は端末2になりすまして、r3とCert2を送信する。なお、Cert2はあらかじめ端末2の通信を盗聴することによって入手しておく。

(5) 端末1は、r12=R(r1、r3)=1 $K12=r12^{S12} \bmod p=1$ を共通鍵として算出する。

(6) 端末3は端末2になりすましてこの'1'を端末1と共有する。

もっとも、この攻撃を困難にするためには、r3を変数と考えたときのR(r1、r3)=c modpの方程式の求解を困難にするような関数R()を定めればよい。

次に、第２図は、一方向通信を行う本発明の認証機能付き鍵配送方法の一実施例を示す。この実施例においても、図の簡略化のため共通の鍵をもつことを希望する２つの端末１、２のみを示す。端末１は秘密情報ｘ１を保持する発信側端末、端末２は秘密情報ｘ２を保持する受信側端末である。

証明書発行フェーズは従来例と同じであり、証明書は公開リストに登録されているとする。ただし、システムで１つの一方向性関数ｆ（）を定めて公開しておく。一方向性関数は入力から出力値は容易に求めることができるが出力値から入力値を求めることが非常に困難である関数である。

鍵配送フェーズについて図を用いてステップ毎に説明する。

ステップ(1)：

端末１は乱数ｒ１を生成し、次の式で配送情報Ｚ１を計算する。

$$Z1 = g^{r1} \bmod p$$

ステップ(2)：

端末１は公開リストを参照して端末２の証明書Cert２を知り、次式に基づきｙ２を得る。

$$h(Cert2) = y2 \| ID2$$

ステップ(3)：

ｙ２を用いて次の計算を行い共有鍵Ｋ１２を得る。

$$u1 = y2^{r1} \bmod p$$

$$S12 = y2^{x1} \bmod p$$

$$K12 = u1 + S12 \bmod p$$

ステップ(4)：

端末１は共有鍵Ｋ１２を一方向性関数ｆ（）に入力して配送情報ｖ１を求める。

$$v1 = f(K12)$$

ステップ(5)：

端末１は、Cert１．Ｚ１、ｖ１を端末２に配送する。

ステップ(6)：

端末２は、端末１からの配送データCert１から、ｙ１を得る。

$$h(Cert1) = y1 \| ID1$$

ステップ(7)：

ｙ１を用いて次の計算を行い共有鍵Ｋ２１を得る。

$$u2 = Z1^{x2} \bmod p$$

$$S21 = y1^{x2} \bmod p$$

$$K21 = u2 + S21 \bmod p$$

ステップ(8)：

端末２は共有鍵２１を一方向性関数ｆ（）に入力して配送情報ｖ２を求める。

ステップ(9)：

端末２は上記作成したｖ２と端末１から送付されたｖ１を比較して、一致する場合のみこれを採用する。

なお、

$$u1 = y2^{r1} \bmod p = g^{x2 \times r1} \bmod p$$

$$= Z1^{x2} \bmod p = u2$$

$$S12 = y2^{x1} \bmod p = g^{x1 \times x2} \bmod p$$

$$= y1^{x2} \bmod p = S21$$

が成り立つため、Ｋ１２＝Ｋ２１となる。

この一方向通信バージョンの例では、受信者は送信者と同じ値のｕ２を得るために自身の秘密情報を用いる必要がある。また、送信者側もＳ１２を得るためには自身の秘密情報が必要である。従って、受信者がｖ１を検査し、同じセッション鍵を共有できたことで送信者の認証を行う。

ここで、第３の端末が端末１になり澄まし、その時のセション鍵を求めたとしても、第３の端末と正規の端末２の間で鍵の共有が成立しないため受信者側でセッション鍵が削除され、攻撃は成り立たない。

なお、この実施例ではセッション毎に異なるｕ１＝ｕ２と固定の秘密鍵Ｓ１２＝Ｓ２１から、加算を用いて共有鍵を生成しているが、あらかじめ定められたものであればこの演算はどのようなものであってもよい。ただし、トータルの計算量の削減のためには加算又は乗算を用いればよい。

発明の効果

以上の説明から明らかなように第１の発明は、第１の従来例と比べ通信回数が１パス分だけ減少していると共に、共有鍵を得るための計算量もべき乗剰余演算３回の第２の従来例に比べて演算１

回分少なくて済む。このため、認証機能付きの鍵配送を、通信回数並びに共有鍵を得るための計算量を少ない状態で行うことができるといった効果がある。

第2の発明によれば、秘密情報を知らない第3者と正規の端末は鍵を共有し得ないので、正規の端末は共有鍵をチェックすることによって相手の不正を検出することができる。また、万が一、セッション鍵とその時の通信路上のデータを求められたとしても、これにより秘密の共有鍵（固定値）を求めるためには、その時の送信者の発生した乱数又は受信者の秘密情報を知る必要がある。

さらに万が一、秘密の共有鍵が求められたとしても正規の端末1、2間の通信路上のデータからそのセッションの共有鍵を求めることはできない。

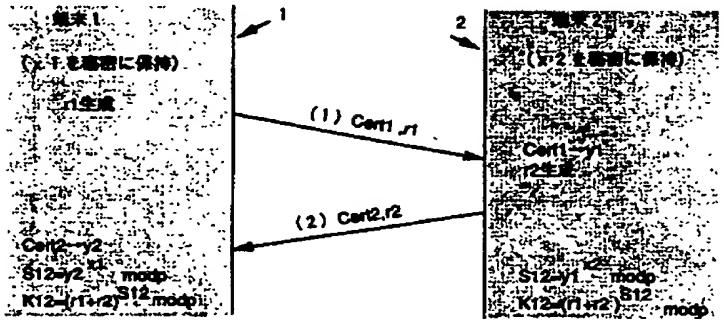
従って、第2の発明は盗聴やなりすまし攻撃に対し、何重にも防御処理を施した安全な方法であるといえる。

4．図面の簡単な説明

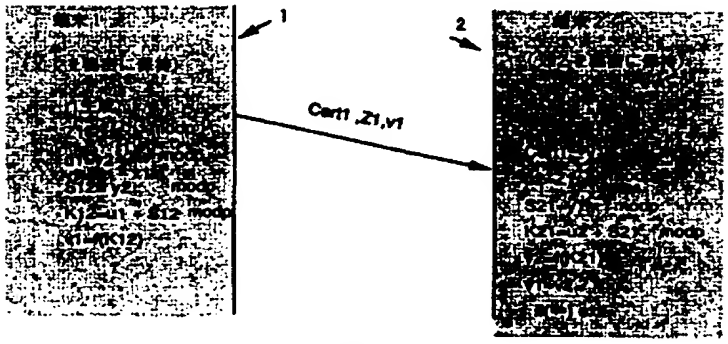
第1図は第1の発明（双方向通信バージョン）の一実施例における鍵配送時の手順説明図、第2図は第2の発明（一方向通信バージョン）の一実施例における鍵配送時の手順説明図、第3図は双方向通信バージョンの第1の従来例における鍵配送時の手順説明図、第4図は双方向通信バージョンの第2の従来例における鍵配送時の手順説明図、第5図は一方向通信バージョンの従来例における鍵配送時の手順説明図である。

1…端末1、2…端末2。

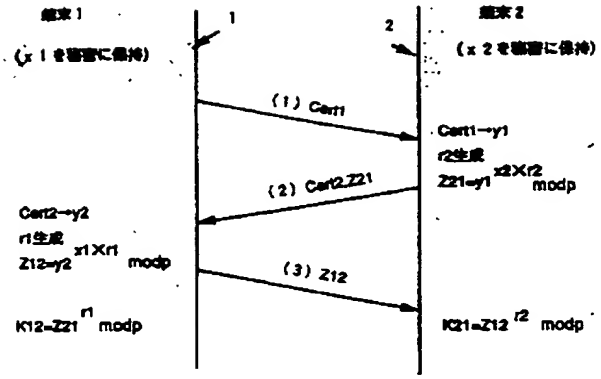
代理人　：　弁理士　中島　司朗



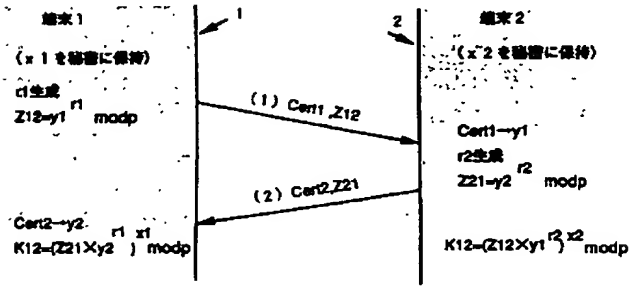
第1図



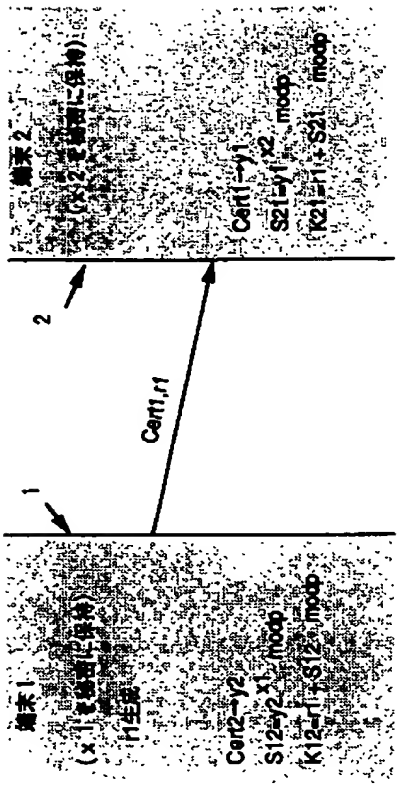
第2図


端末1
(x1を秘密に保持)
1
2
端末2
(x2を秘密に保持)
(1) Cert1
Cert1→y1
r2生成
Z21=y1^x2×r2 modp
(2) Cert2,Z21
Cert2→y2
r1生成
Z12=y2^x1×r1 modp
(3) Z12
K12=Z21^r1 modp
K21=Z12^r2 modp

第3図


端末1
(x1を秘密に保持)
1
2
端末2
(x2を秘密に保持)
r1生成
Z12=y1^r1 modp
(1) Cert1,Z12
Cert1→y1
r2生成
Z21=y2^r2 modp
(2) Cert2,Z21
Cert2→y2
K12=(Z21×y2^r1)^x1 modp
K12=(Z12×y1^r2)^x2 modp

第4図


端末2
(x2を秘密に保持)
Cert1→y1
S21=y1^x2 modp
K21=r1+S21 modp
2
Cert1,r1
1
端末1
(x1を秘密に保持)
r1生成
Cert2→y2
S12=y2^x1 modp
K12=r1+S12 modp

第5図